THE OPEN PALLET POOL.

We are increasingly noticing the sending of phishing e-mails. How do you protect yourself against phishing e-mails?

Phishing emails are fraudulent messages that often try to trick you into revealing personal or business information. Phishing emails can be the key for hackers to access and control your personal or business accounts. This in turn leads to further fraud or security breaches. A common feature is that the displayed sender hides a different email address. Here are some steps to identify phishing emails:

1. Check the sender's email address

If you retrieve your emails via a browser, you can view the source text of the HTML email. In most e-mail programs, it is sufficient to move the mouse pointer over the sender line without clicking on it. In this way, you can determine whether a different address is stored.

Please ensure that the sender is spelled correctly. The European Pallet Association e.V. only uses the following e-mail combination Firstname.Surname@epal-pallets.org . We will never ask you to enter confidential data by e-mail.

EPAL will confirm requests and changes to sensitive company data, such as bank details, via your secure area in My EPAL!

2. Pay attention to the following warning signals:

- **Fake e-mail sender address**: Check whether the specified address matches the official the official e-mail address of EPAL.
- **Urgent need for action**: Phishing emails often try to exert pressure by claiming that immediate action is required.
- **Spelling and grammatical errors**: Watch out for incorrect language or unprofessional wording.
- **Links to fake websites**: Take a close look at the links before you click on them. They often lead to fake sites. These websites are deceptively genuine and look like the official websites of well-known companies. As soon as the user enters their data, it is transmitted to the attackers.
- **Requesting confidential data**: Be careful if you are asked to enter personal information such as passwords or account details.
- **Be careful with attachments:** Check the e-mail first before opening an attachment.

If you have identified an incoming e-mail as a fraud attempt, do not click on the left and do not open any attachments. If possible, right-click on the email, then click on "Block" and confirm with "Block sender" and delete the email.

By following these instructions, you can better protect yourself against phishing attacks. If you have any doubts as to whether an e-mail is a genuine e-mail from the European Pallet Association e.V. or an attempted scam, please contact us. Please forward us a complete e-mail (including address details) to info@epal-pallets.org .

We will support you in checking the e-mail and get back to you as soon as possible.